IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,
Plaintiffs,

v.

BRIAN KEMP, ET AL.,
Defendants.

DECLARATION OF DUNCAN BUELL IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

Civil Action No. 1:17-CV-2989-AT

Pursuant to 28 U.S. § 1746, I, Duncan A. Buell, declare under penalty of perjury that the following is true and correct:

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I have been asked by counsel for Donna Curling, Donna Price, and Jeffrey Schoenberg to offer observations regarding the security of the DRE systems and their use in Georgia elections, based on my years of experience in the field of election security. I previously submitted an Affidavit on behalf of the Plaintiffs in this matter (Dkt. No. 15-2 Ex. G), a copy of which has been attached hereto as **Exhibit A**.

2. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University

of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell. My qualifications and experience are more fully set forth in **Exhibit A**.

3. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

4. I base the opinions in this Declaration on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

5. I have also used as a basis for my opinions a review of the documents regarding the KSU CES hack in Spring 2017, including those attached to the Affidavit of Logan Lamb (Dkt. No. 258-1 pp. 138-369).

6. In my experience working with electronic voting systems, one of the fundamental issues I have seen is the assumption among election officials that because a computer is being used, there is an additional level of protection that ensures accuracy and propriety of voting procedures. However, this is a false comfort. All software has inherent flaws, although some flaws are greater than others. Thus, it is important to understand the risks involved, to utilize programs that present the least risk, and, critically, to have in place procedures that further mitigate any risk present in the program selected. The prudent computing professional will always have in place procedures and practices to recover from the errors that we must always assume will happen. Based on my review of the material provided to me in this case to date, there is no indication that Georgia has followed these standard guidelines.

7. As a general matter, the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world with any interest or experience in election systems. The Diebold system has been scrutinized a number of times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has

been successful. As a result, there are serious, well-known risks associated with the use of the Diebold DREs used in Georgia.

8. One of the primary risks of the system is manipulation through the insertion of malware. Given the manner in which Georgia operates its elections through a central server, one need only access this central server in order to inject malicious code that could cause "disruption" (errors or failures) or "corruption" (the altering, addition, or deletion of votes) to a significant number of machines.

9. It is important to keep in mind that any malware injected does not have to be immediately executable, but can be written so as to execute only under certain conditions, perhaps only on Election Day, or otherwise tailored to meet the goals of the person attacking the system. Unfortunately, there is a wide array of coding techniques that could be employed to launch a targeted attack on a particular election, such as implementing a code to alter every one out of every 20 votes. In my experience, any sophisticated attack will likely involve multiple layers of code that are not only undetectable during an attack, but are "self-deleting" after they have been fully executed.

10. The risks of the DRE system software are exacerbated by the fact that there is no ability to audit results of any given election. As a result, in those instances in which there is a breach in protocol (whether intentional through one of

the methods set forth above or otherwise), there is often no way to determine the impact. The DRE system is able to count what was recorded, but there is no way to know if the vote as recorded by the DRE was what the voter intended. Thus, an attack is often undetectable, and the question of whether an attack actually had an impact on the election necessarily goes unanswered.

11. In addition to these general vulnerabilities, I understand that, as of late-2016, Georgia's central GEMS server was running a particular version of Drupal software that had well-known security vulnerabilities. Drupal is an open-source content-management system (CMS), meaning that it is a free product that has been modified by many people and used by many others. Over time, different versions of this software have presented different vulnerabilities. The specific version used by Georgia was subject to a vulnerability that resulted in what was aptly named Drupalgeddon, as it contained a well-known vulnerability to SQL Injection, which Drupal itself announced in October 2014.[1] Drupal warned that "a vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL injection .... This vulnerability can be exploited by anonymous users."[2]

---

[1] https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-core/2014-10-15/sa-core-2014-005-drupal-core-sql

[2] *Id.*

12. SQL injection refers to a method of attack whereby a malicious user can insert code into forms on a website in order to have the website return a wide array of (often sensitive) data. SQL injection is the common culprit behind many well-known data breaches, including the breach of the Illinois voter registration system that occurred in June 2016, as a result of which approximately 90,000 voter registration records were estimated to have been compromised.[3]

13. Based on my review of documents, I understand that officials at the Center for Election Systems ("CES") at Kennesaw State University, who at the time were responsible for the state's central server, were made aware in October 2016 of the Drupal vulnerability that permitted ready access to Georgia voter registration databases, based on the access of information by Logan Lamb. (Dkt. No. 258-1 at 126.) Mr. Lamb appears to have exposed this vulnerability again in February 2017, as it had not been fixed by that time. (*Id.* at 127.)

14. In my experience, the lapse in security that permitted Mr. Lamb to access the server twice before change was implemented is simply inexcusable. It is a basic premise of network management to keep all software versions up to date, to monitor bug and vulnerability news lists so as to learn quickly of bugs and vulnerabilities, and to install any and all software patches or bug fixes as they

[3] https://www.intelligence.senate.gov/sites/default/files/documents/os-ssandvoss-062117_0.pdf.

become available. At the time Mr. Logan accessed the central server in October 2016, the Drupal SQL vulnerability had been reported nearly two years earlier. In my nine years as chair of the Department of Computer Science and Engineering at the University of South Carolina, with a year in that period when I served as Interim Dean of the college, I was the supervisor for the college's network systems administrator. I can attest that monitoring news lists for vulnerabilities was a routine and ongoing activity and that patches and updates were made as soon as they became available and reliable, even at the occasional cost of lost productivity due to small amounts of downtime.

15. The prudent and professional systems administrators, when alerted to the potential of an unknown vulnerability, will know that it is critical to respond quickly in order to validate the risk and take whatever steps necessary to correct the vulnerability. Based on my review of material provided to date, these steps were not taken until March 2017 at the earliest, and to date, I have not seen evidence indicating that the proper corrective steps have been taken.

Columbia, South Carolina
Dated: August 7, 2018

DUNCAN A. BUELL

EXHIBIT A

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of the petition to void the June 20, 2017, election and to prohibit further use of Georgia's current DRE voting system..

2. In my opinion, the Diebold electronic voting system used in Georgia is vulnerable both to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has been successful.

3. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system. Indeed, the recent reports from the Kim Zetter article for *Politico* seem to demonstrate that the KSU CES has been either unable or unwilling to address security, privacy, and integrity issues even when they have been privately disclosed to the CES by credible cybersecurity professionals. The fact that the FOIA request of Mr. Garland Favorito yielded only three emails between CES and Mr. Logan Lamb and Mr. Christopher Grayson suggests further that CES might not have been taking seriously the security threats that were pointed out by Lamb and Grayson.

Qualifications and Relevant Employment History

4. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

5. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

6. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics

different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

7. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

8. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

9. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued. When

the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well. I have obtained and analyzed the data from the 2012, 2014, and 2016 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, North Carolina, Pennsylvania, and Texas.

Basis for My Opinions

10. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

11. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

The Diebold Election System Was Unacceptable for Use in the CD6 Election Held 20 June 2017

12. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of

Feldman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the "standard" Diebold election system, even operated in intended conditions, have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

13. Evidence indicates that the April 18 and June 20 Special Elections were conducted using a "non-standard" customized Diebold DRE voting system, with an unusual configuration, not tested by a federally accredited laboratory.

14. Even more alarming is the fact that the CES server containing crucial election programming files was known to be open to entry and manipulation in August 2016, and this glaring security problem had not been corrected even as late as March 1, 2017.

15. We must assume that the failure to secure the system and its data caused the already unreliable and unfit system unquestionably to be vulnerable to undetected attack. The system must be considered compromised and it is only prudent that the system must be considered to have been compromised from August 2016 through March 2017, and should not be used to conduct a public election.

16. It has been well-established in the computer security world that the Diebold election system, as configured for "standard" use, is unfit for use due to security and reliability concerns. In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold

systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

17. The response from Secretary Kemp has been tepid at best. His letter of June 5, 2017, does not address technical questions, and does not really address the questions posed by the electors of Georgia in their original request to him.

18. To be specific, the report of 18 April 2017, attached to Mr. Gay's email to Merle King, is damning in what it says and what it does not say. What we see as "successes" are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

19. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

20. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the potential damage done by the fact that the CES system was apparently open to attack for an extended period by any determined actor.

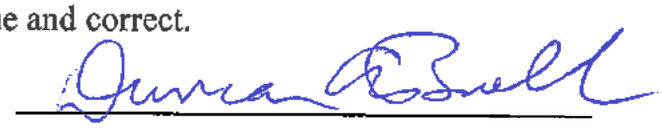
21. Indeed, the report can be read to suggest that the CES was not following some of the most basic security practices taught to all undergraduates in a computer

security course. Issues 1 and 8, under "Opportunities for Improvement", for example, cite a poor understanding of risk and of asset value on a main server and a failure to perform a security assessment. This apparent failure to know and to understand basic principles of security would not be inconsistent with Mr. Lamb's account that sensitive data was still openly available months after he had notified CES of this major security problem.

22. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally or state certified, and provided to the citizens of Georgia an election system in which they can be confident. For these reasons, the voting system in use cannot reasonably be approved as "safe and accurate for use" as required by Georgia statute.

23. For these reasons, I would argue that the Diebold system ought not be used in elections unless and until a complete security analysis has been performed on the software and hardware and a complete verification and integrity check has been made of the databases, including voter registration databases. Nor should the reported results generated by the system be relied on for a determination of the outcome of the June 20 special election.

24. I affirm that the foregoing is true and correct.



DUNCAN BUELL Date

Sworn before me this 29th day of June, 2017, in Columbia, SC.

Rebecca Mayo
NOTARY PUBLIC